



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/875,095	06/07/2001	Kristofer Skantze	3782-0134P	7701
2292	7590	12/22/2004	EXAMINER	
BIRCH STEWART KOLASCH & BIRCH PO BOX 747 FALLS CHURCH, VA 22040-0747			KLIMACH, PAULA W	
			ART UNIT	PAPER NUMBER
			2135	
DATE MAILED: 12/22/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/875,095	SKANTZE, KRISTOFER	
	Examiner	Art Unit	
	Paula W Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 01 November 2001.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-26 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) Claim(s) _____ is/are allowed.
6) Claim(s) 1-26 is/are rejected.
7) Claim(s) _____ is/are objected to.
8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 11/01/01.
4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: ____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-2, 4-6, 14-15, 17-19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dorenbos (5,751,813) in view of Sekendur (5,852,434).

In reference to claims 1 and 14, Dorenbos a system and method for secure wireless transmission of information from a sender to a receiver, comprising: a sending device arranged for obtaining a message and a receiver identity (column 4 lines 43-47); encryption means for encrypting the message to be transmitted (Fig. 3 and column 5 lines 18-22); a transmission channel from the sending device (part 317 Fig. 3) to a receiving device for transmitting the encrypted information to the receiving device (column 5 lines 46-60); decryption means for decrypting the information in the receiving device (column 5 lines 47-48); display means for presenting the message to the receiver (part 127 Fig. 1);

Although Dorenbos suggests a form of displaying the received information (part 127 Fig. 1), however Dorenbos does not disclose the use of a secure note in which a pattern is connected to a receiving device.

Sékendur discloses a system and method of digitizing a position related code for indicating coordinates on a surface (abstract). The secure note disclosed by Sekendur is the data surface (column 5 lines 1-3) and therefore a piece of paper; and the pattern (column 5 lines 22-

25) on the secure note is connected to a receiver; the receiver being processor or computer where the signal from the CCD is sent to (column 5 lines 9-14). The stylus is used to enter data in writing such as address information.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a system for digitizing a position related code for indicating coordinates on a surface as in Sekendur for IO in the system of Dorenbos. One of ordinary skill in the art would have been motivated to do this because it would enable the user to input hand written data.

In reference to claims 2 and 15, wherein said pattern is a portion of an absolute position pattern coding absolute positions, and at least one position of an absolute position receiving address.

Dorenbos does not disclose the use of an absolute position determination device and therefore does not disclose a pattern is a portion of an absolute position pattern coding absolute positions, and at least one position of an absolute position receiving address.

Sekendur disclose a method and system of absolute position determination of the position of a stylus (abstract). Sekendur discloses a pattern is a portion of an absolute position pattern coding absolute positions, and at least one position of an absolute position receiving address (column 5 lines 22-40).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a system for digitizing a position related code for indicating coordinates on a surface as in Sekendur for IO in the system of Dorenbos. One of ordinary skill in the art would have been motivated to do this because it would enable the user to input hand written data.

In reference to claims 4 and 17, wherein the message is obtained by using an absolute position pattern coding absolute positions.

Dorenbos does not disclose the use of an absolute position determination device and therefore does not disclose a pattern is a portion of an absolute position pattern coding absolute positions, and at least one position of an absolute position receiving address.

Sekendur disclose a method and system of absolute position determination of the position of a stylus (abstract). Sekendur further disclose writing or drawing on the surface causes coordinates to be scanned and therefore the writing (message) is obtained by using an absolute position pattern coding absolute positions (using the coordinates of the systematically coded writing surface; column 5 lines 22-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a system for digitizing a position related code for indicating coordinates on a surface as in Sekendur for IO in the system of Dorenbos. One of ordinary skill in the art would have been motivated to do this because it would enable the user to input hand written data.

In reference to claims 5 and 18, wherein the encryption means is arranged to encrypt the message in the sending device by a symmetric key and that the decryption means is arranged to decrypt the message in the receiving device by the same key (column 1 lines 10-20).

In reference to claims 6 and 19, wherein the symmetric key has been agreed upon in advance and is stored in the sending device and the receiving device.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to agree upon the symmetric key in advance and store it in the sending device and the receiving device. One of ordinary skill in the art would have been motivated to do this

because the key is supposed to be kept secret therefore it cannot be transmitted between the device and therefore must be stored in the device in advance when no transmission is necessary.

In reference to claim 22, further comprising a verification means for identification of the sender to the sending device: and/or identification of the receiver to the receiving device, said verification means being arranged to use identification measures, such as Pin-code, optical, sound, vibration, heat, speed, angle, times pressure, acceleration, absolute coordinate, handwritten signature, voice recognition, fingerprint sensor, or other biometric means (column 2 lines 64-67).

Claims 3 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dorenbos and Sekendur as applied to claim 15 above, and further in view of Jalili (6209104 B1).

Dorenbos does not disclose receiving address is obtained by transmitting said one position to a database, in which the absolute position code is associated with said one receiving address and using said receiving address for the transmission.

Although Sekendur discloses determining the position coordinates (abstract), Sekendur does not disclose transmitting said one position to a database, in which the absolute position code is associated with said one receiving address and using said receiving address for the transmission.

Jalili discloses transmitting said one position to a database, in which the absolute position code is associated with said one receiving address and using said receiving address for the transmission (Fig. 8 parts 808 and 810 and column 6 lines 4-20).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the position information associated with an address for transmission for the receiving address. One of ordinary skill in the art would have been motivated to do this because sending coordinates to the server instead of the graphics reduces the amount of data that needs to be transmitted.

Claims 7-13, 20-21, and 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dorenbos and Sekendur as applied to claim 18 above, and further in view of Schneier.

In reference to claims 7 and 20, Dorenbos discloses the message being encrypted, however Dorenbos does not disclose the symmetric key is added to the message after encryption with the symmetric key; the encryption means is arranged to encrypt at least the symmetric key by a public key of an asymmetric key having a private key and a public key and belonging to the receiver; code is connected to at least one the decryption means is arranged to decrypt the symmetric key by the private key of the receiver in the receiving device; and the decryption means is arranged to use the symmetric key for decrypting the message.

Schneier discloses the symmetric key is added to the message after encryption with the symmetric key; the encryption means is arranged to encrypt at least the symmetric key by a public key of an asymmetric key having a private key and a public key and belonging to the receiver; code is connected to at least one the decryption means is arranged to decrypt the symmetric key by the private key of the receiver in the receiving device; and the decryption means is arranged to use the symmetric key for decrypting the message (page 51 paragraph 1-2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a asymmetric key to encrypt a symmetric key and attach the key to the message as taught by Schneier in the system of Dorenbos. One of ordinary skill in the art would have been motivated to do this because it is a common key-exchange protocol.

In reference to claims 8 and 21, wherein the encryption means is arranged to encrypt the already encrypted symmetric key in the sending device by a private key of an asymmetric key having a private key and a public key and belonging to the sender, the receiving device is arranged to obtain the sender public key, such as from the sending device or a separate server; and the decryption means is arranged to decrypt the symmetric key by the public key of the sender in the receiving device and by the private key of the receiver.

Dorenbos does not disclose encrypt the already encrypted symmetric key in the sending device by a private key of an asymmetric key having a private key and a public key and belonging to the sender, the receiving device is arranged to obtain the sender public key, such as from the sending device or a separate server; and the decryption means is arranged to decrypt the symmetric key by the public key of the sender in the receiving device and by the private key of the receiver.

Schneier teaches encrypt the symmetric key in the sending device by a private key of an asymmetric key having a private key and a public key and belonging to the sender, the receiving device is arranged to obtain the sender public key, such as from the sending device or a separate server; and the decryption means is arranged to decrypt the symmetric key by the public key of the sender in the receiving device and by the private key of the receiver (page 49). Schneier

further teaches multiple encryption and therefore encrypting the already encrypted session key (page 367).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use multiple encryption algorithms on the same message as in Schneier in the system of Dorenbos. One of ordinary skill in the art would have been motivated to do this because if one of the receipt of the message or the sender of the message does not trust the algorithm of the other party, with this method both algorithms may be used and the encryption will be as strong as the strongest algorithm.

In reference to claims 10 and 23, further comprising encryption key generation means for obtaining a random seed for generating encryption key by means of the verification means during the identification step.

Although Dorenbos disclose encrypting messages using keys, Dorenbos does not disclose key generation means for obtaining a random seed for generating encryption key by means of the verification means during the identification step.

Schneier disclose the generation of random number for use as keys, which are used for identification as pass-phrases (page 423 and 173-174).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate random number keys as in Schneier in the system of Dorenbos. One of ordinary skill in the art would have been motivated to do this because random bit strings provide good keys.

In reference to claims 11 and 24 further comprising: encryption key generation means for obtaining a random seed for generating an encryption key during the step of obtaining the message.

Dorenbos does not disclose key generation means for obtaining a random seed for generating an encryption key during the step of obtaining the message.

Schneier discloses key generation means for obtaining a random seed for generating an encryption key during the step of obtaining the message (page 173).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate random number keys as in Schneier in the system of Dorenbos. One of ordinary skill in the art would have been motivated to do this because random bit strings provide good keys.

In reference to claims 9, 12, and 25, wherein the sending device is arranged to generate a sender private key and sender public key pair, and is arranged to use a random seed obtained using a physical parameter of the sender, such as handwritten signature recognition, fingerprint information, or movement of the sending device or of the sending device, such as acceleration speed, time, vibration etc.

Dorenbos does not disclose the sending device is arranged to generate a sender private key and sender public key pair, and is arranged to use a random seed obtained using a physical parameter of the sender, such as handwritten signature recognition, fingerprint information, or movement of the sending device or of the sending device, such as acceleration speed, time, vibration etc.

However Schneier discloses a random seed obtained using a physical parameter (page 173).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate random number keys as in Schneier in the system of Dorenbos. One of ordinary skill in the art would have been motivated to do this because random bit strings provide good keys.

In reference to claims 13 and 26 wherein the sender public key is added to the message, unencrypted, as sender identification.

Dorenbos does not disclose the sender public key is added to the message, unencrypted, as sender identification.

Schneier discloses the key used as identification, pass-phrase, (page 174), further Schneier teaches a key added to the message (page 51).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate random number keys as in Schneier in the system of Dorenbos. One of ordinary skill in the art would have been motivated to do this because random bit strings provide good keys.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, November 29, 2004



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2130